DEPARTMENT OF INSURANCE
STATE OF CALIFORNIA
45 Fremont Street, 21st Floor
San Francisco, California 94105

RH-01018269 **December 4, 2001**

INITIAL STATEMENT OF REASONS

PRIVACY OF NONPUBLIC PERSONAL FINANCIAL AND MEDICAL RECORD INFORMATION

INTRODUCTION

California Insurance Commissioner Harry W. Low proposes the adoption of Title 10, Sections 2689.1-2689.24, California Code of Regulations, regarding privacy of information gathered by licensees in connection with insurance transactions.

The purpose of these regulations is to implement, interpret and make specific the provisions of California Insurance Code, Division 1, Part 2, Chapter 1, Article 6.6, Sections 791-791.27 and the privacy provisions of Gramm-Leach-Bliley Financial Services Modernization Act [1] (GLBA), 15 U.S.C., Subchapter I, Sections 6801-6810.

California Insurance Code (CIC) Sections 791-791.27, the Insurance Information and Privacy Protection Act enacted in 1980, establishes standards for the collection, use, and disclosure of information gathered in connection with insurance transactions. This legislation adopted the National Association of Insurance Commissioners' (NAIC) 1982 model legislation, developed with input from state regulators and representatives of industry, producers and consumers to facilitate uniform privacy standards among states.

Title V of GLBA (15 U.S.C. Sections 6801-6810) requires various federal agencies and state insurance authorities to enact regulations respecting the privacy of customers and protecting the security and confidentiality of nonpublic personal information. Federal agencies have adopted implementing regulations for financial institutions subject to the jurisdiction of federal regulators. GLBA expressly permits states to enact privacy protections greater than those required by GLBA or by federal regulations.

Currently, there are no regulations that govern the collection, use, disclosure, and safeguarding of information under Sections 791-791.27 of the Insurance Code. The lack of regulations has led to some confusion on the part of licensees regarding their obligations under California and federal law. These proposed regulations are intended to clarify the procedures implementing the privacy protections set forth in the Insurance Code and to comply with the GLBA mandate, consistent with the public policy of providing maximum privacy protection permitted under these laws.

[1] P.L. 106-102, signed November 12, 1999.

SPECIFIC PURPOSE OF THE REGULATONS AND NECESSITY

The specific purpose of each regulation and the rationale for the Commissioner's initial determination that each regulation is reasonably necessary to carry out the purpose for which it is proposed is set forth below.

Article I: General Provisions

Section 2689.1 Authority and Purpose

Section 2689.1 provides authority for the promulgation of these regulations and clarifies that these regulations are intended to implement provisions of CIC §§791-791.27 and to comply with the GLBA mandate. The rationale for adopting this regulation is to clearly indicate to the public the legal authority for this rulemaking and what provisions of the Insurance Code and federal law will be implemented.

Section 2689.2 Scope

Section 2689.2 clarifies that these regulations apply to nonpublic personal information gathered by licensees about policyholders, claimants and beneficiaries of insurance products or services used primarily for personal, family, or household purposes, and sets forth some of the circumstances under which a business policy might be subject to these regulations. Adopting this regulation is necessary to set forth clearly the persons and circumstances to which the regulations apply to assist affected persons in understanding provisions of the statute and regulations to ensure compliance.

Section 2689.3 Duty of Confidentiality and Care

Section 2689.3 makes clear that licensees have an affirmative duty to protect the confidentiality of nonpublic personal information consistent with CIC §§791-791.27, GLBA privacy provisions, and all other applicable laws regarding the privacy or confidentiality of nonpublic personal information. Adoption of this regulation is necessary to clarify the obligations imposed on licensees by these laws.

Section 2689.4 Definitions

Section 2689.4 defines several key terms referred to in these regulations that are not defined in CIC §§791-791.27 and might otherwise be unclear to affected persons. Adoption of this regulation is necessary for the public to understand provisions of the statutes and regulations. Section 2689.4(a) requires that notices of information practices be "clear and conspicuous." This section adopts the same standards for a "clear and conspicuous" notice as those in federal regulations applicable to federal agencies except it also requires that notices be understood by those with an average eighth grade educational level and achieve a minimum Flesch Score of 50. The rationale for this regulation is to achieve consistency and uniformity in privacy standards between California and federal law. The added standards are reasonably necessary to ensure that consumers will understand a licensee's information practices.

Section 2689.4(b) defines "collect" consistent with the definition in federal regulations applicable to federal agencies. The Insurance Code and GLBA establish standards for the collection of nonpublic personal information in connection with insurance transactions. The rationale for this regulation is to assist consumers in understanding these provisions and to achieve uniformity in privacy standards between California and federal law.

Section 2689.4(c) defines "consumer" in similar terms to GLBA except that this regulation includes claimants and beneficiaries as examples of consumers not included in GLBA because it focused on financial institutions. This is an important definition because it clarifies the scope of the statutes. The rationale for adoption of this regulation is to assist licensees in understanding the statutes and regulations to ensure compliance.

Section 2689.4(d) defines "customer relationship" and provides examples of when a consumer is or is not a customer in accordance with federal regulations adopted by applicable federal agencies. GLBA requires that licensees provide notice of their information practices at the time of establishing a customer relationship and then annually. This regulation is necessary to clarify those provisions so that affected persons are knowledgeable about their rights and obligations.

Section 2689.4(e) defines "financial institutions" and Section 2689.4(f) defines "financial product or service" according to similar standards in GLBA and federal regulations. Since the Insurance Code focuses on licensees subject to its jurisdiction, it does not define the terms. Consequently, the terms may be unclear to licensees. However, GLBA imposes privacy obligations on "financial institutions," including insurers. The rationale for this regulation is to assist affected persons in understanding applicable privacy laws and achieve consistency and uniformity between California and federal law.

Section 2689.4(g) defines "nonaffiliated third party" and Section 2689.4(h) defines "control" consistent with standards in GLBA and federal regulations adopted by applicable federal agencies. CIC §§791-791.27 and GLBA establish required standards for notice and disclosures of nonpublic personal information to affiliated and nonaffiliated third parties. The distinction is significant and this regulation clarifies the distinction so that consumers and licensees understand their rights and obligations. The rationale for this regulation is to achieve uniformity in privacy standards between California and federal law.

Section 2689.4(i) defines "publicly available information" in similar terms as the federal regulations adopted by applicable federal agencies. This is an important definition because CIC §§791-791.27 and GLBA establish standards governing the treatment of nonpublic personal information. This regulation specifies the type of information that is not covered by these privacy provisions so that affected persons understand their rights and obligations. The rationale for this regulation is to facilitate uniformity of privacy standards between California and federal law.

Article II: Privacy Notices; Opt Out Notices for Financial Information

Section 2689.5 Initial Privacy Notice

Section 2689.5 sets forth standards under which an initial privacy notice may be delivered within a reasonable time after a customer relationship is established, paralleling federal regulations applicable to federal agencies. The purpose of this regulation is to clarify procedures for the initial privacy notice so that licensees understand their obligations to ensure compliance. Adoption of this regulation is necessary to comply with the GLBA mandate and achieve uniformity of privacy standards between California and federal law and regulations.

Section 2689.6 Annual Privacy Notice
Section 2689.6 adopts an annual notice requirement for customers. CIC §791.04 provides that a licensee meets requirements for notice of information practices, in the case of a policy renewal, if notice is delivered within the previous 24 months. However, GLBA (15 U.S.C. Section 6803) requires annual notice to a customer, as defined in federal regulations. Since the federal standard of annual notice is stricter, federal law supersedes. The rationale for this regulation is to conform to the mandated federal standard.

Section 2689.7 Information to be Included in Privacy Notices
Section 2689.7 clarifies information requirements for privacy notices by adopting similar standards contained in federal regulations adopted by applicable federal agencies. Often consumers are unaware of the information that is collected about them in connection with insurance transactions and do not know the uses made of the information collected. Without such information, they cannot make informed choices based on privacy concerns they may have. The purpose of this regulation is to assist the consumer in obtaining such information. The rationale for this regulation is to achieve uniformity between California and federal law. For clarification, this section also makes clear that written authorization before a licensee discloses nonpublic personal information must comply with standards set forth in CIC §791.13(a).

Section 2689.8 Form of Opt Out Notices and Opt Out Methods
Section 2689.8 clarifies opt out procedures and information requirements to be followed when a licensee is required to provide an opt out notice. CIC §791.13 sets forth the general rule that a licensee is prohibited from disclosing a consumer's nonpublic personal information without prior written authorization, subject to certain exceptions. One of the exceptions, CIC §791.13(k), permits disclosure to a nonaffiliated third party for marketing purposes, but requires that a consumer be given an opportunity to indicate he or she does not want personal information disclosed (opt out) and has given no such indication. The statute does not specify opt out procedures. However, federal regulations adopted by applicable federal agencies set forth standards for a clear and conspicuous notice that explains the right to opt out, provide examples of opt out methods, and set forth procedures for handling an opt out direction by joint consumers. This regulation adopts the federal standards. The purpose of this regulation is to make clear how to exercise a consumer's right to opt out in applicable circumstances. Adoption of this regulation is necessary to achieve uniformity in privacy standards between California and federal law.

Section 2689.9 Revised Privacy Notices
Section 2689.9 clarifies procedures for revised privacy notices. CIC §791.04 sets forth standards for notice of information practices but does not specifically set forth standards for revised notices. However, federal regulations applicable to federal agencies requires a clear and conspicuous revised notice that accurately describes a licensee's information policies and practices and provides for a new opt out form when applicable. This regulation adopts similar standards. Since federal regulations only specify a reasonable opportunity to opt out, this section interprets the provision by giving consumers 45 days to opt out of the disclosure. The rationale for this regulation is that 45 days is a reasonable amount of time for a consumer to take action and a reasonable waiting period for the licensee before disclosing nonpublic personal information about the consumer.

Section 2689.10 Delivery of Notices
Section 2689.10 clarifies standards and provides examples of adequate methods to deliver privacy notices. CIC §791.04 requires notice of information practices but does not specify methods of delivery of notices. However, federal regulations adopted by applicable federal agencies set forth standards of reasonable expectation of delivery and provide examples of both reasonable and unreasonable expectations. This regulation adopts similar standards and examples to ensure that such notification reaches consumers. The rationale for this regulation is to achieve uniformity of privacy standards between California and federal law and regulations.

Article III: Limits on Disclosures of Medical Record Information
Section 2689.11 Disclosure of Medical Record Information
Section 2689.11 clarifies the limits and conditions on disclosure of medical record information. CIC §791.13 requires a licensee to obtain prior written authorization before disclosing nonpublic personal information, defined in CIC §791.02(s) to include medical record information, subject to certain exceptions. Since GLBA was focused on financial institutions, GLBA is silent on the treatment of medical record information. The rationale for this regulation is to make clear the limits on disclosure of medical record information.

Article IV: Standards for Safeguarding Nonpublic Personal Information
Section 2689.12 General Provisions
GLBA (15 U.S.C. Sections 6801, 6805(b) and 6807) specifically requires the establishment of standards to safeguard nonpublic personal information. Section 2689.12 clarifies that the regulations in Article V are intended to establish procedures to develop and implement administrative, technical, and physical safeguards to ensure the security and confidentiality of nonpublic personal information. The regulations are similar to the federal regulations promulgated by the applicable federal agencies. Adoption of this regulation is necessary to harmonize California law and the GLBA.

Section 2689.13 Definitions
Section 2689.13 defines "customer information systems" and "service provider" consistent with standards in the NAIC 2000 model legislation, developed to track GLBA requirements for safeguarding nonpublic personal information. The purpose of defining these terms is to assist licensees in understanding the safeguarding requirements in these regulations. Adoption of this regulation is reasonably necessary to achieve consistency between states and uniformity between California law and federal law.

Section 2689.14 Information Security Program
Section 2689.14 clarifies the requirements of an information security program for licensees. CIC §§791-791.27 and GLBA establish broad standards for safeguarding nonpublic personal information, but do not specify the process. The rationale for this regulation is to comply with the GLBA mandate and achieve consistency between California law and federal law.

Section 2689.15 Objectives of Information Security Program Section 2689.15 establishes similar objectives for an information security program as in GLBA. The rationale for this

regulation is to comply with the GLBA mandate and achieve consistency between California law and federal law.

Section 2689.16 Assess Risk
Section 2689.16 implements the safeguarding process mandated by GLBA by setting standards to assess the threat of risk to the integrity of customer information and information systems. The standards parallel the standards set forth in NAIC's 2000 model legislation. Although CIC §791-791.27 and GLBA established standards for the safeguarding of nonpublic personal information, the statutes did not specify the process. This regulation implements, interprets and makes specific those provisions. The rationale for this regulation is to comply with the GLBA mandate and achieve consistency between California law and federal law.

Section 2689.17 Manage and Control Risk
Section 2689.17 implements the safeguarding process mandated by GLBA by setting standards to manage and control risks to the integrity of customer information and information systems. The standards parallel the standards set forth in NAIC's 2000 model legislation. Although CIC §791-791.27 and GLBA established standards for the safeguarding of nonpublic personal information, the statutes did not specify the process. This regulation implements, interprets and makes specific those provisions. The rationale for this regulation is to comply with the GLBA mandate and achieve consistency between California law and federal law.

Section 2689.18 Service Providers
Section 2689.18 implements the safeguarding process mandated by GLBA by setting standards to oversee service providers. The standards parallel the standards set forth in NAIC's 2000 model legislation. Although CIC §791-791.27 and GLBA established standards for the safeguarding of nonpublic personal information, the statutes did not specify the process. This regulation implements, interprets and makes specific those provisions. The rationale for this regulation is to comply with the GLBA mandate and achieve consistency between California law and federal law.

Section 2689.19 Adjust the Program
Section 2689.19 implements the safeguarding process mandated by GLBA by setting standards to monitor and adjust the information security program. The standards parallel the standards set forth in NAIC's 2000 model legislation. Although CIC §791-791.27 and GLBA established standards for the safeguarding of nonpublic personal information gathered in connection with insurance transactions, the statutes did not specify the process. This regulation implements, interprets and makes specific those provisions. The rationale for this regulation is to comply with the GLBA mandate and achieve consistency between California law and federal law.

Section 2689.20 Enforcement
CIC §§791-791.27 and GLBA impose a number of obligations upon licensees. The Insurance Code and 15 U.S.C., Section 6805(6) authorize the Insurance Commissioner to enforce these obligations. The rationale for Section 2689.20 is to clarify that the Insurance Commissioner is responsible for audit compliance and enforcement of these standards and regulations, consistent with the statutes.

Article V: Additional Provisions

Section 2689.21 Protection of Fair Credit Reporting Act

Section 2689.21 clarifies that CIC §§791-791.27 does not modify, limit, or supersede the operation of the federal Fair Credit Reporting Act (FCRA) (15 U.S.C. §§1681 et seq.). Since disclosures of certain information may give rise to obligations under FCRA, GLBA (15 U.S.C. Section 6806) expressly protects the operation of FCRA. This regulation adopts a similar standard. The rationale of this regulation is to achieve uniformity in privacy standards between California and federal law.

Section 2689.22 Nondiscrimination

Section 2689.22 clarifies that a licensee is prohibited from discriminating against a consumer for withholding disclosure authorization by denying the consumer an insurance product or service. CIC §791.13 requires prior written authorization before disclosure of nonpublic personal information, setting forth certain exceptions, including the requirement of an opt out notice to consumers before disclosing information to nonaffiliated parties for marketing purposes. It does not specify consequences when a consumer does not provide authorization or exercises the option of opting out against disclosure. The rationale for this regulation is to protect the consumer's exercise of privacy rights.

Section 2689.23 Severability

Section 2689.23 clarifies that each section of the regulations is severable. The rationale for this regulation is consistency with customary legal protections in the eventuality that a section or portion of a section or its applicability to any person or circumstance is held invalid by a court.

Section 2689.24 Effective Date

Section 2689.24 clarifies that the Insurance Commissioner intends the effective date of these regulations to be 30 days after filing with the Secretary of State. The rationale for this regulation is consistency with the rulemaking process to allow a standard reasonable transition period before the regulations take effect .

Appendix A-Sample Clauses

Appendix A provides sample clauses to assist licensees in drafting privacy notices, explaining a consumer's right to opt out of disclosures, and describing its practices to protect the confidentiality and security of customer information.

IDENTIFICATION OF STUDIES

The Commissioner has not relied upon technical, theoretical, or empirical studies or reports in proposing these regulations.

SPECIFIC ACTIONS, PROCEDURES, TECHNOLOGIES OR EQUIPMENT

Adoption of these regulations would not mandate the use of specific technologies or equipment or prescribe specific actions or procedures.

ALTERNATIVES

The Commissioner has determined that no reasonable alternative exists to carry out the purpose for which the regulations are proposed or would be as effective and less burdensome to affected private persons than the proposed regulation.

ECONOMIC IMPACT ON BUSINESS

The Commissioner has initially determined that the proposed regulations will not have a significant adverse economic impact on businesses because they are already required to comply with similar federal requirements of the Gramm-Leach-Bliley Financial Services Modernization Act (15 U.S.C., Subchapter I). The Commissioner invites interested parties to comment on whether the proposed regulations will have a significant adverse economic impact on business.